الإثبات الجنائي في الجرائم الإلكترونية



ذ. مليكة ابوديار: قاضية محامية سابقا بنقابة هيئة المحامين بفاس.
وباحثة في سلك الدكتوراه بكلية الحقوق بمكناس

مقدمة:

إن الإثبات في المواد الجنائية قديم قدم الإنسان، وهو مرتبط بكل جهد قضائي في سبيل اظهار الحقيقة التي تهم المجتمع بأسره، ولا تظهر الحقيقة الا بعد البحث عنها وثبوتها بالأدلة. فالإثبات الجنائي على هذا الأساس هو العصب الرئيسي للحكم الجنائي، اذ فيه وحده يكمن السبب الذي يقود القاضي الى اصدار هذا الحكم بالإدانة أو بالبراءة [1].

وقد أنتجت ثورة المعلومات والتكنولوجيا وتعاظمت أهمية المعلوماتية وقيمتها في عصرنا الحالي الذي أصبح يعرف بعصر تكنولوجيا المعلومات، وسائل جديدة لخدمة البشرية، غير أنها في ذات الوقت فتحت الباب أمام ارتكاب صور من الجرائم لم تكن معروفة سابقا والتي أصبحت تعرف بالجرائم الإلكترونية، بل ترتكب باستخدام التقنية عبر أجهزة الكترونية وشكلت مصدرا وافرا لإشكاليات قانونية هامة بالأخص من ناحية علاقتها بالقانون الجنائي سواء فيما يتعلق بالتكييف القانوني لهذه الفئة من الجرائم، أو من حيث وموضوعها وخصائصها وأشخاصها وأساليب ارتكابها ومدى امكانية الكشف عنها[2]. والأهم هو أن ما تحقق للبشرية من مصلحة عبر الثورة التكنولوجية حقق أيضا ضررا لها وهو ما أسس لانتشار الجرائم الإلكترونية التي تختلف اختلافا جذريا عن أنواع الجرائم الأخرى مع الأخذ بعين الاعتبار أن الضرر الناجم عنها لا يمكن الاستهانة به [3]، مما يطرح التساؤل حول إشكالية الإثبات الجنائي في الجريمة الإلكترونية، وكيفية الحصول على الدليل الإلكتروني حتى يعرض أمام القاضي الجنائي.

ويعد الإثبات بالأدلة الرقمية من أبرز تطورات العصر الحديث في كافة النظم القانونية [4]. ومن هنا تبدو أهمية الإثبات الجنائي بالدليل الرقمي في كون هذا الأخير الوسيلة الوحيدة والرئيسية لإثبات هذه الجرائم

1- محمد أمين الخرشة، مشروعية الصوت والصورة في الاثبات الجنائي دراسة مقارنة، الطبعة الثانية ، دار الثقافة ، عمان الأردن 2015ص21و32
2 - دلخار صلاح بوتاني، الحماية الجنائية الموضوعية للمعلوماتي، دراسة مقارنة، الطبعة الأولى ،دار الفكر الجامعي الإسكندرية 2016،ص13
3 - علي عدنان الفيل، الإجرام الإلكتروني، دراسة مقارنة الطبعة الأولى مكتبة زين الحقوقية،طريق صيدا القديمة لبنان،2011،ص7.
4 - أحمد يوسف الطحاوي، الأدلة الالكترونية في الاثبات الجنائي، دراسة مقارنة، دطبعة، دار النهضة العربية، القاهرة2015،ص4.

ISSN: 7476-2605 ردمد

المستحدثة، وفي كون جل التشريعات التقليدية لا تواكب الإجرام الإلكتروني الذي ما فتئ يتطور مما حدا بالتشريعات الدولية والعربية إلى سن قوانين بالموازاة مع التطور الاجتماعي لبلدها .

وربط الإثبات الرقمي بالقانون الجنائي، يرجع إلى كون هذا القانون يشمل من جهة مجموعة القواعد العامة التي تتعلق بالجريمة ومسؤولية مرتكبيها وأنواع الجزاءات، ومن جهة أخرى يحوي القواعد الخاصة بكل جريمة وما يشملها من جزاء[1]. وهذه الجريمة تشمل العادي والمعلوماتي. وعرف أحد الفقهاء وهو (Mass) هذه الأخيرة بأنها:" الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح". كما ذهب الفقيه الألماني (Tiedemann) الى "أن الجريمة المعلوماتية تشمل كل أشكال السلوك الذي يرتكب باستخدام الحاسب"[2]. وبهذا المفهوم فالجريمة الالكترونية ظاهرة اجرامية فريدة فهي جريمة افتراضية في عالم افتراضي وبآليات افتراضية."[3]

وقد تطور الفكر الانساني في مجال الاثبات الى خمس مراحل تعرف الأولى بالمرحلة البدائية كانت خالية من أي تنظيم قانوني لقواعد الاثبات أو سلطة تختص بتطبيقها وفي المرحلة الثانية اتجه تفكير الجماعات الى الاحتكام الى الآلهة، وقد ساد مذهب الاثبات الديني في هذه المرحلة، وكانت أهم وسائله اليمين، والابتلاء، وهو إجراء يخضع له من يشتبه فيه في ارتكابه جرما معينا للتوصل الى كونه بريئا أو مدينا، والمبارزة القضائية تأخذ صورة الاقتتال الفردي بين الظنين والمدعي. والمرحلة الثالثة كانت هي مرحلة الأدلة القانونية. وهنا ظهرت الجذور الأولى لنظام الأدلة الجنائية. وقد ارتكز نظام الإثبات القانوني في هذه المرحلة على قيام المشرع بتحديد القيمة الإثباتية للقاضي بالنسبة لكل دليل من الأدلة التي يجوز الاستناد عليها في حكمه، بحيث يتقلص دور القاضي الى حد كبير ليحل المشرع بدلا منه .والمرحلة الرابعة تعرف بمرحلة الاقتناع الذاتي، وتمثلت الفكرة الأساسية لهذا النظام في أن المشرع لا يرسم طرقا محددة للإثبات يتقيد بها القاضي ،بل يترك لهذا الأخير حرية الإثبات ومنحه سلطة تقديرية كبيرة في الإثبات ، سواء كان ذلك لقبوله الأدلة أم لتقديرها، ووضع المشرع ضوابط يتعين على القاضي مراعاتها والتقيد بها صيانة للحق وحسن تطبيق القانون. والمرحلة الخامسة هي مرحلة الإثبات العلمي وهي تدل على التطور والتقدم العلمي الكبير الذي تحقق في وسائل الإثبات وما نتج عنه من وسائل علمية حديثة، تستطيع أن تتغلب على كل محاولات الظنين لتضليل العدالة[4]. وهنا تطرح عدة مشاكل قانونية منها: كيف يتم اخراج الدليل من الأجهزة موضوع ارتكاب الجريمة الإلكترونية؟ ومن هو الشخص القائم بهذا الإخراج للدليل؟ وهل هناك أجل قانوني ما بين إخراجه وما بين عرضه على المحكمة؟ وغيرها من المشاكل القانونية التي بلورت الإشكالية التالية.

إن الإشكالية التي يطرحها الموضوع وهي: هل المقاربة القضائية كفيلة بالاستناد على دليل إلكتروني محدد كإثبات جنائي في الجرائم الإلكترونية أم أن الأمر يستدعي تناول هذه الأخيرة من علوم متعددة ومتكاملة؟

1 - محمد العروصي، المختصر في شرح القانون الجنائي المغربي، الجزء الأول، القانون الجنائي العام، الطبعة الثانية ،مطبعة مرجان مكناس2016،ص8.
2– عبد السلام بنسليمان، الاجرام المعلوماتي في التشريع المغربي،،دراسة نقدية مقارنة ، الطبعة الأولى، دار الأمان الرباط2017، ص27.
3 - عبد السلام بنسليمان، الاجرام المعلوماتي في التشريع المغربي ،م س ، ص 29.
4 - محمد امين الخرشة، مشروعية الصوت والصورة في الاثبات الجنائي ، م س،ص22–31.

ISSN: 7476-2605 ردمد

ويظهر كفرض للموضوع بأنه أصبح من الضروري إيجاد ترسانة تشريعية خاصة بالجرائم الإلكترونية تحدد الدليل الإلكتروني وإجراءاته الشكلية – خاصة وأنه دليل فني وليس مادي كما في الجرائم التقليدية – كإثبات جنائي يعرض أمام القاضي الجنائي وتحدد فيها الفصول أنواع الجرائم وعقوباتها. وحتى يستساغ فهم الفرضية في ارتباط بالإشكالية سيتم التعرض للموضوع عبر دراسة مقارنة بين التشريع المغربي والأمركي والفرنسي والإمارات العربية المتحدة والمملكة العربية السعودية والسودان والأردن من خلال شقين وهما:

أولا: دور القاضي الجنائي في وسائل الإثبات للجريمة الإلكترونية

ثانيا: دور السياسة الجنائية في الحد من الجريمة الإلكترونية

أولا: دور القاضي الجنائي في وسائل الإثبات للجريمة الإلكترونية

يعد الإثبات الجنائي بالأدلة الرقمية من أبرز تطورات العصر الحديث في كافة النظم القانونية وهو يتمتع بصفة الحداثة، ومعلوم ان نظام الإثبات الجنائي تحكمه قرينة البراءة كلما تطرق للدليل الشك ، مما يطرح التساؤل حول مقبولية الدليل الرقمي في إثبات الوقائع الجنائية[1] من جهة وحول مشروعية الأخذ به أمام القاضي الجنائي من جهة أخرى .

أ: وسائل الإثبات الجنائي وأهميتها في الجريمة الإلكترونية

يثير التطور العلمي والتكنولوجي في العصر الحاضر تساؤلات كثيرة على الفكر القانوني، وتضفي على مشكلاته القديمة مشكلات جديدة، و أصبح الدليل العلمي من المسائل التي تحظى باهتمام بالغ في العصر الحديث [2]،ويعد كل من المعاينة والتفتيش والشهادة من أهم وسائل جمع الأدلة ولكل منهم قواعده يتم اتباعها بالرغم من أن التساؤل يثور حول جدوى هذه الوسائل فيما يتعلق باستخلاص الدليل الإلكتروني، ومدى مشروعيتها في حالة تواجد الدليل العلمي .

1: تعريف الإثبات الجنائي وأهميته

بحكم ما للإثبات من أهمية في الوصول إلى الحقيقة وتحقيق العدل، ورغم الصعوبة التي قد يصادفها القاضي الجنائي سيما ما يتعلق بالإثبات بالأدلة الرقيمة، التي تعد من الأمور الصعبة عليه الإلمام بتقنياتها، فإن كل هذا وذاك فرض مقدما تعريف الإثبات الجنائي وبيان أهميته.

يراد بالإثبات دعم الادعاء بالحجة. ويقال أثبت الشيء اثباتا: عرفه حق المعرفة[3]. ومن سائغ القول فإن الإثبات هو التنقيب عن الدليل وتقديمه وتقديره لاستخلاص السند القانوني للفعل في الدعوى[4]. والإثبات قديم قدم الانسان وهو مرتبط بكل جهد قضائي في سبيل إظهار الحقيقة التي تهم المجتمع بأسره؛ لأن الجريمة تمثل اعتداء على الجماعة، ووسيلة المجتمع في الكشف عن الجريمة، وإظهار الحقيقة هي الدعوى الجنائية التي

1 - أحمد يوسف الطحطاوي، الأدلة الالكترونية ودورها في الاثبات الجنائي، دراسة مقارنة، د طبعة ،دار النهضة العربية ،القاهرة ، 2015ص2و3و4.
2 - محمد أمين الخرشة، مشروعية الصوت والصورة في الاثبات الجنائي–دراسة مقارنة– الطبعة الأولى ،دار الثقافة عمان الأردن، 2011ص35.
3 - خليل الجر ومحمد خليل الباشا وهاني أبومصلح ومحمد الشايب، المعجم العربي ،لاروس،د طبعة، مطبعة هيريسي بارس ،فرنسا 1973ص19 .
4- أحمد يوسف الطحطاوي، الأدلة الالكترونية ودورها في الاثبات الجنائي،م س،ص7.

تعد همزة بين الجريمة المرتكبة والعقوبة، والتي تهدف الى تحويل الشبهات القائمة الى حالة من اليقين القضائي[1]. والإثبات أو الدليل الإلكتروني كما عرفه رأي في الفقه:" بأنه الدليل المأخوذ من أجهزة الحاسب الآلي ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، ويتم تقييمها في شكل دليل يمكن اعتماده أمام القضاء" [2].

وتمثل قواعد الاثبات الجنائي أهمية خاصة، اذ إن الحق موضوع التقاضي يتجرد من كل قيمة اذا لم يقم الدليل على الواقعة التي يستند إليها، فالدليل هو عصب الواقعة[3] ولكي يتحقق الدليل اللازم للإثبات فانه لابد من جمع عناصر التحقيق والدعوى، وتقديم هذه العناصر الى سلطة التحقيق الابتدائي ، وإذا أسفر هذا التحقيق عن دليل أو أدلة ترجح معها ادانة الظنين قدمته الى المحكمة، ومرحلة المحاكمة هي أهم المراحل لأنها مرحلة الجزم بتوافر دليل أو أدلة يقتنع بها القاضي بإدانة الظنين والا حكم ببراءته[4]، ومن هنا يتضح أن الإثبات في المادة الجنائية من أهم الأعمدة التي يقوم عليها صرح العدالة الجنائية برمتها وتبتدئ أهمية نظام الإثبات بل خطورته البالغة – وخصوصا على المتابع بخرق القانون الجنائي– أمام القضاء الذي بمجرد وضع القضية بين يديه خصوصا خلال مرحلة دراسة القضية ومناقشتها ، العمل بكل تجرد ونزاهة على الوصول الى الحقيقة واليها وحدها[5].

2: وسائل الإثبات الجنائي

لقد أفرز التطور العلمي والتكنولوجي تغير التواصل بين الأفراد من الشكل البسيط ،كالرسائل والبرقيات الى نمط يرتكز على السرعة والفنية العالية بوسائل تقنية جديدة [6] عبر شبكة الأنترنت مثل الوسائل السمعية والمرئية والبريدية والى مواكبة هذه الوسائل انضمام الخبرة التقنية إلى علم الخبرة المتميز بتصنيف التعامل مع موضوع الدعوى من حيث ضرورة الاستعانة بالمختصين في مجال النزاع [7] وقد ثار جذل فقهي حول قبولها في الاثبات وسيتم التطرق الى هذه الوسائل من خلال كل من المعاينة والتفتيش والشهادة والبصمة الرقمية أو الآثار المعلوماتية ومدى مواكبتها للوسائل الحديثة أعلاه.

1.2: المعاينة

في جميع الأحوال عند تلقي بلاغ عن وقوع جريمة إلكترونية، وبعد التأكد من البيانات الضرورية في البلاغ يتم الانتقال الى مسرح الجريمة لمعاينته، ومسرح الجريمة الإلكترونية يختلف طبعا عن الجريمة التقليدية، ودون الخوض في أوجه الخلاف فإن البعض يرى أن أهمية المعاينة تتضاءل في الجريمة الإلكترونية، وذلك لندرة

1 - محمد أمين الخرشة، مشروعية الصوت والصورة في الاثبات الجنائي ،مرجع سابقص21.
2 - عبد السلام بنسليمان، الاجرام المعلوماتي في التشريع المغربي ،م س ،ص140.
3 - أحمد ضياء الدين، مشروعية الدليل الالكتروني في المواد الجنائية، كلية الحقوق جامعة عين شمس، د طبعة،،مجموعة أحكام النقض1984 ،ص 359.
4 - محمود محمود مصطفى، الاثبات في المواد الجنائية في القانون المقارن، الجزء الأول، الطبعة الأولى ،مطبعة جامعة القاهرة، ، 1978،ص3.
5- عبد الواحد العلمي ، شرح قانون المسطرة الجنائية ، الجزء الثاني، الطبعة الأولى، مطبعة النجاح الجديدة 2000، ،ص 280.
6 - زروق يوسف، حجية وسائل الاثبات الحديثة، رسالة دكتوراه في القانون الخاص، جامعة أبو بكر بلقايد ،تلمسان، كلية الحقوق والعلوم السياسية، 2012–2013 ص 88.
7 - هشام فريد رستم، الجوانب الاجرائية للجرائم المعلوماتية، دراسة مقارنة ، د طبعة، مكتبة الآلات الحديثة، أسيوط 1994ص 141.

ISSN: 7476-2605 ردمد

تخلف آثار مادية عقب ارتكاب هذه الجريمة ،كما أن طول الفترة بين وقوع الجريمة أو إرتكابها وبين اكتشافها يكون له التأثير السلبي على الآثار الناجمة عنها بسبب العبث أو محو أو تلف تلك الآثار[1].

ويطرح هذا الوضع الذي نص عليه قانون المسطرة الجنائية المغربي[2]، سؤال أهمية المعاينة في الجريمة المعلوماتية على اعتبار أن هذه الأخيرة لا تترك أدلة مادية في الواقع، اذ يقوم الجاني بالعبث بها سواء بالحذف أو التغيير أو غيرها من الأفعال المنصوص عليها قانونا ،ناهيك أن الجريمة الإلكترونية في أغلب الأحيان تكون غير تلبسية الأمر الذي يؤكد ضعف أهمية المعاينة فيها وهو الأمر الذي يتساءل فيه عن حدود ضابط الشرطة القضائية أو قاضي التحقيق في التقاط المكالمات والاتصالات المنجزة بوسائل الاتصال عن بعد[3] كما أن المادة 108 من قانون المسطرة الجنائية المغربي المذكور قد سكتت عن تحديد لحظة التقاط البيانات والمعطيات المرتبطة بالاتصالات المنجزة عن بعد[4].

2.2: التفتيش والشهادة

والتفتيش في مدلوله القانوني بالنسبة للجرائم الإلكترونية لا يختلف عن مدلوله السائد في فقه الإجراءات الجنائية ، فهو إجراء من إجراءات التحقيق تقوم به سلطة مختصة لأجل الدخول الى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات وتخزين ومخرجات لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبة وتشكل جناية أو جنحة ، والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبتها الى مرتكبها[5] .

وإذا كان للتفتيش مدلولا واحدا سواء تعلق الأمر بالجريمة العادية أو الجريمة والإلكترونية؛ فإن تطبيق هذا الاجراء على هذا الصنف الأخير من الإجرام يثير العديد من الصعوبات التي تحول دون تحقيق الغاية من الحصول على الأدلة المتعلقة بالجريمة موضوع التفتيش نظرا للصعوبات التي تطرحها الطبيعة الافتراضية للجريمة الإلكترونية، وبالتالي الآثار المترتبة عليها.

وتجدر الإشارة في هذا الصدد الى أن المواثيق الدولية تمنع إكراه الظنين على الشهادة على نفسه أو الاعتراف بأي شيء من شأنه إدانته[6]، ويطرح التساؤل بهذا الشأن بالوضعية التي يتم فيها إلزام الشخص بإعطاء الكود السري لحاسوبه ثم يتبين بعد التفتيش والتحريات أنه بريء من التهمة المنسوبة إليه، فهل يعتبر

---

1 - هشام فريد رستم ، الجوانب الاجرائية للجرائم المعلوماتية، م س، ص59.

2 - نص الفصل 57 من قانون المسطرة الجنائية المغربي رقم 22.01 المنشور بالجريدة الرسمية عدد5078 بتاريخ 27 ذي القعدة 1424 الموافق (30يناير2003) على " أنه يجب على ضابط الشرطة القضائية الذي أشعر بحالة تلبس بجنحة أو جناية أن يخبر بها النيابة العامة فورا وأن ينتقل في الحال الى مكان ارتكابها لاجراء المعاينات المفيدة"

3 - وقد نصت اتفاقية بودابست في المادة 21 منها الى أن التقاط هذه البيانات يتم بشكل فوري أي لحظة انجاز الاتصال أو ارسال المعطيات عبر النظام المعلوماتي.

4 - عبد السلام بنسليمان، الاجرام المعلوماتي في التشريع المغربي ،م س ، ص147و 149.و152

5 - أحمد يوسف الطحطاوي، الأدلة الالكترونية ودورها في الاثبات الجنائي، دراسة مقارنة، م س ، ص 137

6 - وقد نص على هذا الأمر العهد الدولي للحقوق المدنية والسياسية صراحة في مادته 14وفق ما يلي :"لكل متهم بجريمة ألا يكره على الشهادة على نفسه أو على الاعتراف بذنب".

ISSN: 7476-2605 ردمد

هذا الدخول غير مشروع ويترتب عليه تطبيق مقتضيات الفصل 3- 607 من القانون الجنائي؟[1] إلا أن الصعوبة المطروحة عمليا تدور حول انعدام التنظيم القانوني للتفتيش الإلكتروني حتى بعد صدور القانون الجنائي المغربي في صيغته المحينة في13مارس 2018 [2].

وبخصوص الشهادة فهي لا تختلف في مدلولها عن تلك المتعلقة بالجريمة الإلكترونية، إذ يبقى أمر سماع الشهود متروك لفطنة المحقق، ومرتبط بظروف التحقيق وما تسفر عنه. والأصل أن يطلب الخصوم من يرون من الشهود، وللمحقق أن يدعو للشهادة من يقدر أن لشهادته أهمية، وله سماع أي شاهد يتقدم من تلقاء نفسه.

والشاهد في الجريمة المعلوماتية هو ذلك الشخص الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي[3]، والذي تكون لديه معلومات جوهرية وهامة لازمة للولوج في نظام المعالجة الآلية للبيانات، اذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله، ويطلق على هذا الشاهد اسم الشاهد المعلوماتي وذلك تمييزا له عن الشاهد التقليدي[4].

3.2: البصمة الرقمية أو الآثار المعلوماتية

البصمة الرقمية هي تلك الأدلة التي تترك أثرا دون أن يكون الشخص راغبا في وجودها. ويسمى هذا النوع من الأدلة بالآثار المعلوماتية الرقمية. فمستخدم النظام المعلوماتي يترك آثارا بسبب تسجيل الرسائل المرسلة منه أو المرسلة إليه، وكافة الاتصالات التي تمت من خلال النظام المعلوماتي وشبكة الاتصالات. إلا أن هذا النوع من الأدلة لم يعد أساسا للحفظ من طرف من صدر عنه. بحكم أن الوسائل التقنية الخاصة تمكن من ضبط هذا النوع ولو بعد فترة زمنية من نشوئها، فالاتصالات التي تتم عبر المنظومة المعلوماتية المرتبطة بشبكة الاتصالات، وكذا المراسلات الصادرة من الشخص أو التي يتلقاها، يمكن ضبطها بواسطة تقنية خاصة بذلك. ومثاله أن يتواصل أحد الأشخاص عبر البريد الإلكتروني مع غيره لتحريضه بطريقة غير مباشرة على تنفيذ بعض الأعمال التخريبية في بلد معين وذلك بتزويده ببعض الصور التخريبية في أحد البلدان، مما يجعل تلك الصور تسجل بطريقة عرضية على الحاسب الآلي.

وتبرز أهمية التمييز بين هذين النوعين من خلال كون النوع الأول يعمد الى حفظه للاحتياج به. وبذلك فقد أعد سلفا كوسيلة لإثبات بعض الوقائع، بحكم قلة إمكانية فقدانه. كما يكون من السهل الوصول إليه.

1 - عبد السلام بنسليمان، الاجرام المعلوماتي في التشريع المغربي ،م س ، ص154و157و158.

2 - نص القانون الجنائي المغربي على معاقبة مرتكب الجرائم الالكترونية الواردة في الفصل 1-447 على عقوبة بالحبس من ستة أشهر الى ثلاث سنوات مع غرامة نافذة من (2000) درهم الى(20.000) درهم وفي الفصل 2-447 على عقوبة من سنة الى ثلاث سنوات مع غرامة نافذة من (2000)درهم الى (20.000)درهم بينما الفصل 3-447 نص على معاقبة مرتكب الأفعال المشار اليها في الفصلين المذكورين في حالة عود من سنة الى خمس سنوات وغرامة من (5000)الى (50.000) درهم . وللاطلاع على الأفعال المرتكبة انظر مجموعة القانون الجنائي المغربي في صيغته المحينة في 13 مارس 2018.

3 - ويمكن أن يكون الشاهد الشاهد ضابط الشرطة القضائية أو الخبير المختص كل منهما تقنيا وفنيا بمخرجات الأجهزة الالكترونية واعادة دبلجتها على اقراص قصد عرضها على أنظار القضاء.

4 - أحمد يوسف الطحطاوي ، الأدلة الالكترونية ودورها في الاثبات الجنائي، دراسة مقارنة، م س ، ص140.

أما النوع الثاني من الأدلة الالكترونية فيكون الحصول عليه عن طريق اتباع تقنيات خاصة لا تخلو من الصعوبة والتعقيد؛ لأنه لم يعد أصلا كي يكون أثرا لمن صدر عنه[1] ويذكر منها على سبيل المثال الملفات التي تم حذفها من النظام والتي تتم استعادتها بعد ذلك من طرف المختصين والخبراء.

ب: سلطة القاضي الجنائي في قبول الدليل وشرعيته

إن مجرد الحصول على الدليل الرقمي كإثبات في المادة الجنائية وتقديمه للقضاء لا يكفي لاعتماده كدليل للإدانة، إذ الطبيعة الفنية الخاصة للدليل الرقمي تمكن من العبث بمضمونه على نحو يحرف الحقيقة، دون أن يكون في قدرة غير المتخصص إدراك ذلك العبث، ولذلك تثور فكرة الشك في مصداقيتها كأدلة للإثبات الجنائي، علما أن نسبة الخطأ الفني في الحصول على الدليل الرقمي نادرة للغاية، إلا أنها ومع ذلك تظل ممكنة ويحدث هذا إما بسبب الخطأ في استخدام الأداة المناسبة في الحصول على الدليل الرقمي كخلل في الشفرة أو استخدام مواصفات خاطئة وإما بسبب خطأ في استخلاص الدليل، ويرجع ذلك الى اتخاذ قرارات لاستخدام الأداة تقل نسبة صوابها عن (100%) ويحدث هذا غالبا بسبب وسائل اختزال البيانات أو بسبب معالجة البيانات بطريقة تختلف عن الطريقة الأصلية التي تم تقييمها.[2] لذا يقوم القاضي الجنائي بدور هام اتجاه الدليل الجنائي، أي بما يتحقق له من اقتناع منه.

1: دور القاضي الجنائي في البحث عن الدليل وقبوله وتقديره

يملك القاضي الجنائي من الوسائل القانونية التي تمكنه من البحث عن الحقيقة وإقامة الدليل عليها وتكملة النقص أو القصور الموجود في الأدلة المطروحة عليه– سواء طلب أطراف الدعوى منه ذلك أم لم يطلبوا– وله أن يطلب أي دليل يراه مناسبا لإظهار الحقيقة كتعيين خبير واحد أو أكثر في النازلة لسد أي فراغ في إجراءات الدعوى في جميع مراحلها، وذلك بغض النظر عن مسلك الأظناء في هذا الصدد. ولا يختلف دور القاضي الجنائي في البحث عن الدليل الجنائي التقليدي عن دوره في البحث عن الدليل الإلكتروني، إلا أنه في الحالة الأخيرة يوجب عليه القانون الاستعانة بأهل الخبرة في هذا الشأن حتى لا يتم فقد الدليل أو العبث بمخرجاته[3].

وارتباطا بما سبق فقد أخذ المشرع بمبدأ حرية الإثبات، حيث أمد القاضي الجنائي بحرية واسعة في الإثبات، جعله حرا في قبول الأدلة من عدمها. فقبول الأدلة يعتبر الخطوة الإجرائية التي يمارسها القاضي اتجاه الأدلة المقدمة في الدعوى قبل تقديرها، لكن هذا الأمر فيما يتعلق بالدليل الجنائي المادي. أما بالنسبة للدليل الجنائي الرقمي فهو يختلف كليا عن الدليل الجنائي المادي، لأنه يكون في وسط افتراضي ولذلك فمجرد الحصول على الدليل الرقمي وتقديمه للقضاء لا يكفي لاعتماده كدليل للإدانة، إذ الطبيعة الفنية للدليل الرقمي

---

1 - سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، ماجستر في العلوم القانونية، جامعة الحاج لخضر باتنة، كلية الحقوق والعلوم السياسية 2012–2013 ص 129

2 - أحمد يوسف الطحطاوي ،الأدلة الالكترونية ودورها في الاثبات الجنائي، دراسة مقارنة، م س ،ص 222 و 224.

3 - بينت المادة 194 من ق م ج المغربي الجهة الي لها صلاحية تعيين الخبراء، موضحة بانه:" يمكن لكل هيئة من هيئات التحقيق أو الحكم كلما عرضت مسألة تقنية أن تأمر بإجراء خبرة إما تلقائيا وإما بطلب من النيابة العامة أو من الأطراف.."

ISSN: 7476-2605 ردمد

تمكن من العبث بمضمونه على نحو يحرف الحقيقة، دون أن يكون في قدرة غير المتخصص إدراك ذلك العبث كما سبق ذكر ذلك مما يمكن معه القول أن الشك في الدليل الرقمي لا يتعلق بمضمونه كدليل وإنما بعوامل مستقلة ولكنها تؤثر في مصداقيته. ولاشك أن الخبرة تحتل دورا مهما في التثبت من صلاحية الدليل الرقمي، في حالة بقاء الشكوك التي تؤثر على عقيدة القاضي بخصوص سلامة الدليل الذي سبق خضوعه لاختبارات فنية بعد تقديمة أمام القاضي الجنائي، وبذلك يتضح أنه اذا كانت الغلبة بالنسبة لإثبات الجرائم الإلكترونية ستكون للإثبات بالقرائن والخبرة، فان ذلك سيزيد من أهمية الدليل العلمي في الإثبات الجنائي، وفي ذات الوقت يزيد من أهمية دور القاضي الجنائي في هذا الإثبات بحيث يظل متمتعا بسلطة تقديرية في تقدير هذه الأدلة ، بحسبان أنها قد لا تكون مؤكدة على سبيل القطع، أو قد تكون مجرد إمارات أو دلالات، أو قد يحوطها الشك، وهنا تظهر أهمية هذه السلطة التقديرية التي يجب أن يظل القاضي متمتعا بها، لأنه من خلالها يستطيع إظهار مواطن الضعف في هذه القرائن، ويستطيع كذلك تفسير الشك لصالح الظنين[1].

وعن تقدير الدليل الرقمي، فإنه لا يعود إلا لقاضي الموضوع وحده. فهذه العملية هي جوهر عمل القاضي الجنائي اتجاه ذلك الدليل، فهي عملية ذهنية ، يعتمد فيها القاضي على المنطق، وعلى وعيه وإدراكه بكافة أدلة الدعوى الجنائية، وتمحيصها ثم استنتاج ما تحتويه من أدلة قادرة على خلق اليقين لديه، فالقاضي الجنائي هو في نهاية المطاف الذي يقوم بالتنسيق بين الأدلة المختلفة إثباتا ونفيا، ويستخلص منها في النهاية مجتمعة عقيدته سواء بالبراءة أو بالإدانة.

فأساس الأحكام الجنائية انما هو حرية قاضي الموضوع في تقدير الأدلة القائمة في الدعوى، ما دام بين حكمه أنه لم يقض بالبراءة أو بالإدانة الا بعد أن ألم بتلك الأدلة ووزنها، فلم يقتنع وجدانه بصحتها ، فلا يجوز مصادرته في اعتقاده ولا المجادلة في حكمه ، فقد جعل القانون من سلطة القاضي أن يزن قوة الإثبات، وأن يأخذ بأي بينة أو قرينة يرتاح إليها دليلا للحكم. ومثلما يخضع الدليل الإلكتروني لقواعد معينة تحكم طرق الوصول إليه فانه يخضع لقواعد أخرى للحكم على قيمته التدليلية وذلك يرجع للطبيعة الفنية لهذا الدليل ،فمنها ما هو متعلق بوسائل تقييم الدليل من حيث سلامته من العبث وهذا مناط عرضه على الخبرة ، فبحث مصداقية هذا الدليل من صميم فن الخبير[2]، ومنها ما يعرض لاختبار فني، بغية التأكد من أن هذه الأداة لا تعرض بيانات زائفة حتى يمكن الأخذ بذلك الدليل كأساس لتكوين عقيدة القاضي.

2: شرعية الدليل الإلكتروني في الإثبات الجنائي

ساهم التطور العلمي في تقديم العديد من الوسائل العلمية الحديثة التي تساعد على كشف الجريمة وإظهار الحقيقة، وقد ظهرت من بين هذه الوسائل أجهزة التسجيل الصوتي والصورة ،وتطورت حتى أصبحت سهلة الحمل وسهلة الإستعمال إذ يمكنها ان تلتقط ما يدور في المكان المغلق من أحاديث، وهذه الوسائل الحديثة بقدر ما تساعد السلطات على كشف الجريمة فإنها تمثل تعديا صارخا على الحريات الشخصية وانتهاكا

1 - أحمد يوسف الطحطاوي ،الأدلة الإلكترونية ودورها في الإثبات الجنائي، دراسة مقارنة، م س ،ص232و234.و246

2 - أحمد يوسف الطحطاوي ،الأدلة الإلكترونية ودورها في الإثبات الجنائي، دراسة مقارنة، م س، ص 235 و239.

للكثير من حقوق الانسان اللصيقة به[1] وسيتم التطرق لمشروعية الدليل الإلكتروني في بعض التشريعات الغربية والعربية وفي التشريع المغربي.

1.2: مشروعية الدليل الإلكتروني في بعض التشريعات الغربية والعربية

منذ ثمانينيات القرن الماضي التي شهدت ثورة تقنية المعلومات ،برزت ظاهرة جرمية غير معتادة رافقت خط المسار التاريخي الذي مرت به تقنية المعلومات نشأة وتبلورا وتطورا، فتم توظيف تقنية المعلومات الحديثة في الاحتيال على المصارف واعتراض بطاقات الائتمان وسرقتها واستخدامها غير المشروع، والابتزاز والسطو على البنوك إلكترونيا والتزييف والتزوير والاحتيال الإلكتروني وتدمير الحاسبات البنكية ،ووجد العابثون من ذوي النزعة الإجرامية ضالتهم في استغلال هذه التقنية وتحقيق مآربهم عن طريقها، بدءا من جرائم الاعتداء على حق الانسان في شرفه وسمعته واعتباره ،وحقه في حرمة حياته الخاصة، وفي سلامة الجسم والحياة، مرورا بالجرائم الأخلاقية والإخلال بالآداب العامة ،انتهاء بالإرهاب والتجسس وتهديد أمن الدولة، فقد تحول الانسان إلى هدف من أهداف مجرمي التقنية الحديثة بعد أن أتاحت الثورة الرقمية تحقيق أغلب صور الاعتداء على الأشخاص من جنح بسيطة إلى جنايات كبرى وبأبسط الاساليب.

وهكذا توجهت الأنظار إلى طائفة من الأفعال في بيئة تكنولوجيا المعلومات الحديثة التي تقتضي العمل على خلق إطار قانوني لها ، يقوم على تصنيفها وضبطها وخلق العقوبات الرادعة اللازمة لحماية البشر من تأثير وحماية النشاطات بكافة أنواعها ،ذلك أن التكنولوجيا والقانون متلازمان وكل منهما يخدم الآخر[2] فجرائم تقنية المعلومات الحديثة تعني تأثير هذه التكنولوجيا وأدواتها على القوانين الجزائية .

والولايات المتحدة كانت من بين الدول الأوائل التي أقرت مشروعية الدليل الإلكتروني عن طريق تشريع قوانين لمكافحة جرائم التقنية في مختلف الولايات ويمثل الفصل(18) من قانون الولايات المتحدة التشريع الرئيس لجرائم التقنية الحديثة، وقد استجاب الكونكرس لمشكلة جرائم تقنية المعلومات من خلال سن العديد من القوانين الفدرالية كان أولها قانون الاحتيال وإساءة استخدام الكمبيوتر عام **1984** وتم تعديله عام **1986** من أجل التعامل مع مشكلة "الشيفرة الخبيثة" وغيرها من البرامج التي تهدف الى تغيير أو إتلاف أو تدمير البيانات على نظام الحاسب.

وينص القسم (**1030**) من الفصل (**18**)على عدة أفعال من قبيل الجريمة : كالتوصل غير المصرح به (الدخول) سواء الى الى أحد أنظمة الحاسب للحصول على معلومات خاصة بأموال محمية، أو إلى نظام حاسب خاص بالحكومة الفدرالية الأمريكية، أو الدخول مع نية الاحتيال أو مع تعمد إلحاق أضرار، أو الإتجار الاحتيالي في كلمات السر الحاسوبية وغيرها من المعلومات، أو بث أو تهديد بارتكاب ضرر لأي نظام حاسب محمي عبر الولايات أو للتجارة الأجنبية. ويحظر القسم(**1462**) من الفصل(**18**) من قانون الولايات المتحدة استخدام نظام الحاسب لاستيراد مواد مخلة بالأداب الى داخل الولايات المتحدة الأمريكية، ويجرم

1 - محمد أمين الخرشة ، مشروعية الصوت والصورة في الاثبات الجنائي ، دراسة مقارنة، م س ، ص 121.

2 - حاتم عبد الرحمان، الاجرام المعلوماتي، د ط ، دار النهضة العربية القاهرة 2002 ص 5.

القسم(2251) من الفصل(18) توظيف أي قاصر أو إغرائه للمشاركة في أنشطة جنسية بما فيها خلق وتصوير مواد وبثها لجهات خارجية، أو استخدام نظام الحاسب للإخلال برعاية قاصر بقبول استغلاله مع العلم في إنتاج مواد تنطوي على استغلال جنسي، وغير ذلك من القوانين . كما أصدر الكونكرس عام 2003 قانون مكافحة البريد الإلكتروني غير المرغوب فيه ، ومن بين ما يهدف إليه هذا القانون القضاء على عادة الحصول على عناوين البريد الإلكتروني من مواقع الإنترنت .وتجدر الإشارة إلى أن كل ولاية من الولايات تملك حرية التشريع الخاص بها وليس هناك آلية على مستوى الولايات أو المستوى الفدرالي تتطلب تبني الولايات شكلا أو محتوى محددا لقوانينها ، وقد سنت جميع الولايات قوانين خاصة أو عدلت قوانين العقوبات لديها بما يكفل النص على تجريم أنشطة جرائم تكنولوجيا المعلومات الحديثة مع تباين فيما بينها سواء من حيث صور النشاط المجرم أو من حيث آلية التعامل مع محل الاعتداء[1].

والتجربة الفرنسية في مجال مكافحة جرائم تقنية المعلومات الحديثة ، ليست أقل نضجا من التجربة الأمريكية بل إن فرنسا من أوائل الدول التي تعاملت مع ظاهرة جرائم تقنية المعلومات تعاملا واقعيا بحيث استجابت مبكرة ،وبهذا الخصوص جرم المشرع الفرنسي الهجمات على النظم لمعالجة البيانات وانتهاك حقوق الأشخاص الناشئة عن الملفات أو البيانات الشخصية المعالجة معلوماتيا ،وخرق قواعد التشفير كما نص المشرع الفرنسي على الجرائم الواقعة باستخدام تكنولوجيا المعلومات ، والخاصة بالجرائم الواقعة على الأشخاص كالاعتداء على القصر، من نشر أو تثبيت أو تسجيل أو نقل الصور الإباحية للقاصرين كما جرم فعل القوادة المتعلقة بالقاصرين، باستخدام وسائل تكنولوجيا المعلومات وجرم أيضا تعريضهم للخطر عبر تصنيع أو نقل أو تثبيت أو تداول أي محتوى ذو صفة عنيفة أو إباحية أو ذو طبيعة تسبب ضررا خطيرا لكرامة الإنسان ،من المحتمل أن يشاهدها أو يتداولها قاصر باستخدام تقنية المعلومات الحديثة بالإضافة الى جرائم التهديد والجرائم الواقعة على الأموال، وأيضا الجرائم الواقعة بانتهاك قانون الصحافة أو انتهاك قانون الملكية الفكرية أو تملك أو إدارة المشاركة في مشروع قمار عبر شبكة الأنترنت ،وأيضا الجرائم المتعلقة بانتهاك قانون الصحة العامة بالإتجار بالمخدرات عبر وسائل تقنية المعلومات أو بيع الأدوية بواسطتها دون الحصول على اذن.[2]

وتجدر الاشارة الى أن أغلب التشريعات الأجنبية المقارنة التي جرمت فعل الدخول بدون تصريح إلى النظام المعلوماتي، وسعيا منها إلى تفادي المعنى المادي لفعل الدخول تستعمل كلمة (Access) بدلا من كلمة (Entry) كما هو الحال في المادة 02 من اتفاقية بودابست لسنة 2001 الخاصة بالجرائم المعلوماتية، وكذلك الحال في القانون الفدرالي الأمريكي بشأن جرائم الحاسوب لسنة 1984 في المواد 1030 فقرة أ/1،2 ، كما لجأ القانون الفرنسي الى مصطلح (Access) بدلا من مصطلح (Entrée) في سبيل الابتعاد عن المفهوم المادي لكلمة (الدخول).[3]

1 - علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، دراسة مقارنة، الطبعة الأولى، مكتبة زين الحقوقية، الشياح، طريق صيدا القديمة 2013،ص 139و140الى 143.

2 - علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، دراسة مقارنة، م س ، ص 151و157.

3 - دخار صلاح بوتاني، الحماية الجنائية الموضوعية للمعلوماتية، م س ، ص 191.

ولم تخرج الدول العربية عن سنة التطور بالاهتمام بمشروعية الدليل الإلكتروني. حيث اقتصرت الحركة التشريعية في شأن مواجهة جرائم تقنية المعلومات الحديثة، على كل من دولة الإمارات العربية المتحدة والمملكة العربية السعودية والسودان والأردن، فقد أصدرت دولة الإمارات القانون الإتحادي رقم 2 لسنة 2006 الخاص بمكافحة جرائم تقنية المعلومات الحديثة، وأصدر السودان عام 2007 قانون مكافحة جرائم تقنية المعلومات، كذلك أصدرت المملكة العربية السعودية بتاريخ 2008/01/24 نظامها الخاص بمكافحة جرائم تقنية المعلومات الحديثة، وأصدر الأردن قانون مكافحة جرائم أنظمة المعلومات عام 2010.

2.2: مشروعية الدليل الإلكتروني في التشريع المغربي

وبالنسبة للتشريع المغربي فيمكن القول أن الواقع العملي أثبت أن جريمة الدخول[1] الاحتيالي إلى نظم المعالجة الآلية للمعطيات تعتبر أم الجرائم، فهي الجريمة الأصل التي تتفرع عنها باقي الجرائم الأخرى، والجريمة المعلوماتية فرضت نفسها على المشرع المغربي فكان أن سن قانون 03–07 في سنة 2007 بشأن مكافحة جرائم المس بنظم المعالجة الألية للمعطيات الوارد بمنظومة القانون الجنائي ،وأصبحت المحاكم المغربية مستقرة على اعتبار البريد الإلكتروني "الإيميل" نظاما للمعالجة الآلية للمعطيات [2]

وفي اطار اهتمام المغرب بالجرائم الإلكترونية وفي اطار إسباغ الشرعية للدليل الإلكتروني فقد افتتح في مقر ولاية مراكش المختبر الجهوي لتحليل الآثار الرقمية بتاريخ 12/25/، 2012 وذلك في إطار حرص المديرية العامة للأمن الوطني على مواكبة التطورات التي تعرفها الجريمة بفضل استخدام التكنولوجيا الرقمية ووسائل الاتصال الحديثة، وسيقوم هذا المختبر بالأساس بتجميع الأدلة الرقمية المستعملة في اقتراف الأفعال الإجرامية أو المرتبطة بها واستقرار وتحليل الدعامات الإلكترونية المرتبطة بالجريمة إلى جانب تقديم الدعم التقني الى المحققين والى العدالة فيما يتعلق بالجريمة الالكترونية [3]

وفي نفس السياق نص المشرع المغربي على مشروعية الدليل الإلكتروني عن طريق إصداره الأخير خلال السنة الجارية لمجموعة القانون الجنائي في صيغة محينة بتاريخ 12مارس2018، وقد نص الفصل من447مكرر1 الى447مكرر2 منه [4] على عقوبات حبسية تتراوح بين ستة أشهر الى خمس سنوات وغرامات مالية تتراوح

1 - وجدير بالذكر انه يعاب على التشريعات العربية استخدامها لكلمة (الدخول والاختراق) ،ونفس الشيء في التشريع المغربي الذي استعمل بدوره في مجموعة القانون الجنائي المغربي في الباب العاشر الخاص بالمس بنظم المعالجة الآلية للمعطيات كلمة (دخل) في الفصل 3–607أو (أدخل) في الفصل 6–607 ، ذلك أن الدخول يستخدم في الغالب الأعم للإشارة إلى دخول أماكن محمية أو بدون حماية،أما الاختراق فيشير فقط إلى دخول الأماكن أو الأنظمة المعلوماتية المحمية ببرامج خاصة.

2- وقضت محكمة الاستئناف بالرباط في المغرب في أحد قرارها بتاريخ 2010/01/31 إلى أن النظام المعلوماتي لوزارة الطاقة والمعادن يعتبر فعلا معالجة آلية للمعطيات وقضت في قرارها أن العلبة الالكترونية(Boite Email) لأي نظام معلوماتي هي جزء لا يتجزأ من ذلك النظام، وجدير باستحضار الحكم عدد 215الصادر عن ابتدائية تمارة في 17ماي 2010 والذي تتلخص وقائعه في كون أن شابا استغل واقعة سقوط طائرة أمير خليجي بضواحي مدينة تمارة وأرسل عدة رسائل الكترونية لوكالة الأخبار الإماراتية يقول فيها أنه يحتفظ بالأمير ويطلب فدية لقاء اعطاء معلومات حوله أو اظهار صوره.(للمزيد يرجى الاطلاع على، عبد السلام بنسليمان، الاجرام المعلوماتي في التشريع المغربي ،م س ،ص157 .

3- الجريمة المعلوماتية بالمغرب، منشور على الموقع الالكتروني ساسة بوست https://www.sasapost.com/opinion/cyber-crime-in-morocco/

4 - مجموعة القانون الجنائي المغربي في صيغة محينة بتاريخ 13 مارس2018 منشور على الموقع الإلكتروني لوزارة العدل بالرباط. المغرب.

بين 2.000 درهم الى20.000درهم ونص الفصل447 مكرر3 على عقوبات مضاعفة في حالة ارتكاب الأفعال المنصوص عليها في الفصلين المذكورين أعلاه في حالة العود وفي حالة ارتكاب الجريمة من طرف الزوج أو الطليق أو الخاطب أو أحد الفروع أو أحد الأصول أو الكافل أو شخص له ولاية أو سلطة على الضحية أو مكلف برعايتها أو ضد امرأة بسبب جنسها أو ضد قاصر.

ثانيا: دور السياسة الجنائية في الحد من الجريمة الإلكترونية

يراد بالسياسة الجنائية مجموعة من الإجراءات التي تتخذها الدولة في وقت معين للوقاية من الإجرام ومكافحته ومعاملة المجرمين[1]. وهذه السياسة تتربع على رأس الهرم الذي تكونه العلوم الجنائية بشقيها المعياري والعلمي. وبيان مدى نجاعة السياسة الجنائية في مكافحة الظاهرة الإجرامية لا تستبعد من نطاقها الجريمة الإلكترونية. ووصولا إلى معرفة مدى نجاعة هذه السياسية يحبذ معرفة في المستهل مدلول هذه الجريمة على مستوى القانون الداخلي و الدولي .

أ: مفهوم الجريمة الإلكترونية في القانون الداخلي والدولي

يطرح موضوع الجريمة الإلكترونية اشكالا نظريا على مستوى المفهوم حيث أنه بالرجوع الى الآراء الفقهية نجدها منقسمة فيما بينها الي قسمين أو توجهين، اذ يرى الاتجاه الأول أن الجريمة الإلكترونية لا تشمل سوى الأنشطة الإجرامية التي تستهدف نظم المعالجة الآلية للمعطيات فيما يرى أصحاب التوجه الثاني أن حدود الجريمة المعلوماتية تمتد إلى كل نشاط اجرامي يعتمد المعلوميات أداة من أجل الحصول على منفعة مادية غير مشروعة[2] .

1: مفهوم الجريمة الإلكترونية في القانون الداخلي

لما كان التطور هو سنة الحياة في الكون، وقاعدة أزلية وفطرة الله التي فطر الناس عليها، وأن كل يوم يطل علينا بجديد من المخترعات والمكتشفات وفقا لما أفرزه التقدم العلمي والتقني في شتى مناحي الحياة، وكان الحاسوب هو إحدى هذه الصور وكانت الشبكة العنكبوتية هي إحدى صور الاستخدامات العامة والضرورية لمثل هذه التقنيات الحديثة. فقد حاولت العديد من الأعمال الأكاديمية تعريف الجريمة الإلكترونية، ومع ذلك لا تبدو التشريعات الوطنية مهتمة بتعريف دقيق للمصطلح [3]

على الرغم من التدخل التشريعي المغربي في تجريم الأفعال المكونة للجريمة المنظمة كالإرهاب والإتجار بالبشر وغسيل الأموال أو ما تعلق منها بالمس بالخصوصية تحت مسمى جرائم المس بنظم المعالجة الآلية، إلا أن موضوع الجريمة الإلكترونية يطرح إشكالا نظريا على مستوى المفهوم فقد تم تعريف الجريمة المعلوماتية بأنها

1 - محمد العروصي، المختصر في شرح القانون الجنائي، م س، ص73.
2- عبد السلام بنسليمان، الاجرام المعلوماتي في التشريع المغربي دراسة نقدية مقارنة، م س، ص 24.
3 - أحمد عبد اللاه المراغي، الجريمة الالكترونية ودور القانون الجنائي في الحد منها، دراسة تحليلية تأصيلية مقارنة. الطبعة الأولى المركز القومي للإصدارات القانونية ، القاهرة2017،ص 24.

كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لإرتكابه من ناحية ولملاحقته وتحقيقه من ناحية أخرى.

وقد سار على هذا المنوال فالي علال حيث اعتبر أن الجريمة المعلوماتية تشمل فقط الجرائم التي تكون فيها المعلومات والمعطيات والبيانات والوثائق المضمنة والمخزنة بالحاسوب أو بالنظم المعلوماتية أو بالبرامج التطبيقية أو برامج التشغيل المتعلقة بها موضوعا أو محلا لها، وذلك سواء كانت هذه المعطيات متاحة للجمهور أو سرية يتطلب الأمر توفر شروط معينة لولوجها، وسواء كان مرتكبها مؤهلا لهذا الولوج المشروع بتوفره على كلمات المرور مثلا أو كان يستعمل في ذلك أسلوبا غير مشروع عن طريق الاختراق"[1]

ومهما يكن فان محاولة تحاشي خصوصية الجريمة الإلكترونية تبقى الآليات المعتمدة في ارتكابها هي المعيار المحدد للتمييز بينها وبين الجريمة التقليدية وهي تتميز كظاهرة إجرامية فريدة بخصائص تجعلها ذات طبيعة مختلفة عن الإجرام التقليدي ككونها جريمة عابرة للحدود وتتميز بالصعوبة في اكتشافها لكون مسرحها افتراضي ولا تترك أي آثار محسوسة ولا تترك شهودا يمكن اعتماد شهادتهم ولا أدلة مادية يمكن فحصها.

2: مفهوم الجريمة الإلكترونية على الصعيد الدولي

تعددت التعريفات الخاصة بالجريمة الالكترونية على المستوى الدولي إن على مستوى الفقه أو على مستوى التشريعات سيما المشرع المغربي. وحتى يتأتى الإلمام بمعانيها يستحسن معرفة دلالتها في هذا التشريع الأخير، قبل تمحيص العديد من التعريفات الفقهية للموضوع.

1.2مفهوم الجريمة الالكترونية في التشريع العربي

إن المشرع العربي ومن خلال تناوله للجرائم الإلكترونية باعتبارها جرائم متعددة ومتنوعة ويستعصي حصرها بسهولة، فان الأمر ذاته ينطبق على تعريفها إلا أنه مع ذلك يمكن اعتبارها:

-جميع الأفعال المخالفة للقانون والشريعة والتي ترتكب بواسطة الأنترنت.

-هي الجرائم التي يتم ارتكابها اذا قام شخص باستخدام معرفته بالأنترنت بعمل غير مشروع قانونا ومستخدما الحاسوب كموضوع للجريمة[2].

-وقد عرف نظام المعالجة الآلية للمعطيات في القانون العربي النموذجي الموحد بأنه "كل مجموعة مركبة من وحدة أو عدة وحدات للمعالجة سواء كانت متمثلة في ذاكرة الحاسب وبرامجه أو وحدات الإدخال و الإخراج والإتصال التي تساهم في الحصول على نتيجة معينة"[3].

-ومن جهة أخرى فقد ذهبت بعض التشريعات المتخصصة بجرائم المعلوماتية كالقانونين السوداني والسعودي إلى إيراد تعبير (الالتقاط)[4] وعرفاه بأنه" مشاهدة البيانات أو المعلومات الواردة في اي رسالة الكترونية أو سماعها أو الحصول عليها"، مما يدل أن هذه التشريعات قد عدت الأفعال الواقعة على البيانات

1 - عبد السلام بنسليمان، الاجرام المعلوماتي في التشريع المغربي دراسة نقدية مقارنة، م س، ص 26.

2 - يوسف حسن يوسف، الجرائم الدولية للأنترنت، الطبعة الأولى 2011 المركز القومي للإصدارات القانونية القاهرة ،ص270و271

3 - علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، م س ، ص 31

4 - وتعبير الالتقاط أورده التشريع المغربي في مجموعة القانون الجنائي في صيغة محينة بتاريخ 12 مارس 2018 في الفصول من 1-447 الى3-447 ، والتي سبق التطرق اليها أعلاه.

بهذه الصورة "الالتقاط الذهني" تعد جرائم معاقبا عليها، وهو ما يعني أنها اعترفت بإمكانية حيازة تلك المعلومات بالالتقاط[1].

وعموما فان عامل التطور الزمني الذي واكب تكنولوجيا المعلومات وتكنولوجيا الاتصالات، ساهم بشكل مباشر في تعدد الاصطلاحات والتعريفات التي استخدمت للدلالة والتعريف بالجريمة الإلكترونية– كظاهرة جرمية– والتي بدأت بالظهور مع بدايات ثورة تكنولوجيا المعلومات والتي نمت وتطورت بتطورها الى أن غاية تم معها الوصول الى مرحلة اندماج تكنولوجيا المعلومات وتكنولوجيا الاتصالات[2].

ومن تم يظهر بأن الجريمة الإلكترونية تعد من الجرائم العابرة للحدود التي تقع بين أكثر من دولة، بمعنى أنها لا تعترف بالحدود الجغرافية، وقد قسم فقهاء القانون الجرائم المعلوماتية الى نوعين رئيسيين، جرائم الهدف وجرائم الوسيلة، دون اغفال اختلاف الجرائم من دولة الى أخرى حسب سرعة تطور المجتمعات وبنيتها وحسب قدرة المشرعين في احتواء التقدم الحاصل ضمن اطار قانوني صحيح تحسبا لأي استغلال ضار للتطور التكنولوجي الحاصل في المجتمع:

والنوع الأول وهو ما يسمى جرائم الهدف تكون فيه نظم الكمبيوتر هدفا للجريمة، أي الجرائم التي تستهدف نظام المعلوماتية نفسه، بمعنى أن هدف هذا النمط الإجرامي هو نظام الكمبيوتر وبشكل خاص المعلومات المخزنة داخله بهدف السيطرة على النظام دون أن يدفع الشخص مقابل الاستخدام كسرقة المعلومات أو وقت الكمبيوتر، وتلك الأفعال الاجرامية تتخذ صور متعددة معتمدة على تقنية النظام محل الاعتداء وكذلك على الوسيلة الفنية المتبعة لتحقيق الاعتداء، ويتحقق ذلك عن طريق الدخول غير المصرح به الى النظام والمسمى بالباكر كناية على الاختراق، كما لو توصل أحد المخترقين للدخول الى نظام الحجز في أحد الفنادق لسرقة أرقام الائتمان، أو الدخول والاعتداء على الملكية الفكرية كسرقة الأسرار التجارية واعادة انتاج ونسخ المصنفات المحمية وتحديدا برامج الحاسب والمعلومات المخزنية أو تعديلها أو نسخها وذلك عن طريق زراعة الفيروسات، هذا النمط الاجرامي يسميه جانب من الفقه بفن الحاسب ،أو بالجريمة الإلكترونية.

أما النوع الثاني يسمى بجرائم الوسيلة ،ويعد فيه الحاسب الآلي والأنترنت من أفضل الأسلحة الناعمة في أداء العمل الإجرامي، بدون عنف أو إراقة دماء، وأصبحت نظم الحاسب الآلي والأنترنت طبقا لهذا القسم هي الوسيلة المستخدمة في ارتكاب الجريمة والمعبر عنها بجرائم الوسيلة. ومن أهم صورها: الجرائم التي تقع على الأشخاص وتضم جرائم الأخلاق كالكسب والقذف والتشهير، والجرائم التي تقع عبر الأنترنت مثل الاستغلال الجنسي للأطفال والجرائم التي تقع على الأموال مثل السرقة والنصب وغسيل الأموال وترويج المخدرات والإرهاب الإلكتروني، ويتضح في هذا النمط الاجرامي أن الحاسب هو أداة ارتكاب الجريمة وليس موضوعا لها وأن هذه الجرائم لا تخرج عن كونها تطور في صور ارتكاب الجرائم التقليدية. ويعد موقع الجريمة الإلكترونية من هذا التقسيم مزيجا من جرائم الهدف –فمحل الاعتداء فيها هو المعلومات المخزنة على الحاسب الآلي التي تعد هدفا

1 - عمار عباس الحسيني، جرائم الحاسوب والانترنت، الجرائم المعلوماتية، الطبعة الأولى، مكتبة زين الحقوقية والأدبية 2017،ص132
2 - علي جعفر ، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، م س ، ص76.

ISSN: 7476-2605 ردمد

لهذا الاعتداء–كما أنها من جرائم الوسيلة إذ أن وسيلة ارتكابها هو الحاسب الآلي وأن الاعتداء على المكونات المادية ما هو إلا إحدى صور الجرائم التقليدية أو بوصفها مخازن للمعلومات أو وسيلة معالجتها[1].

2.2 مفهوم الجريمة الالكترونية في الفقه الجنائي الدولي

اهتم فقهاء القانون الجنائي الدولي بدراسة جرائم تقنية المعلومات وقد تعددت المفاهيم التي استخدمت للدلالة على الجريمة الإلكترونية : ومن التعريفات المضيقة لجريمة تكنولوجيا المعلومات الحديثة ما جاء به الفقيه (Merwe) حيث يرى أن هذه الجريمة تتمثل في "الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي". كما يعرفها الفقيه (Tomas.j.Smedinghoff) بأنها "أي ضرب من النشاط الموجه أو المنطوي على استخدام نظام الحاسوب". ويعرفها (مكتب تقييم التقنية بالولايات المتحدة الأمريكية) بأنها: "هي الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا"

وهذا التعريف الذي ارتكز على معيار موضوع الجريمة كأساس للتعريف ،وهو المعيار الذي يعد من أهم المعايير وأكثرها قدرة على إيضاح طبيعة ومفهوم الجريمة محل التعريف.

وعرفها الفقيه (MASS) بأن المقصود بجريمة تكنولوجيا المعلومات يتمثل "بالاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح".

وعرفها الفقيه (Steinschjqlberg) بأنها "أي فعل غير مشروع تكون المعرفة بتقنية الكمبيوتر أساسية لارتكابه والتحقيق فيه وملاحقته قضائيا"

وطبقا لتعاريف الفقهاء سابقة الذكر فان الجريمة الإلكترونية تنحصر في الحالات التي تتطلب قدرا من المعرفة التقنية في ارتكابها[2].

ب: مدى نجاعة السياسة الجنائية في الحد من الجرائم الالكترونية.

أدى ظهور الجرائم الإلكترونية إلى خلق تحديات كثيرة في مواجهة النظام القانوني القائم في العديد من الدول وخاصة في مواجهة قانون العقوبات الأمر الذي يستدعي مواجهة تشريعية باستحداث قوانين أو نصوص خاصة قادرة على احتوائها ومراعاة طبيعتها وخصوصيتها وفي هذا الإطار سيتم عرض هذه المواجهة من خلال التشريع المغربي والدولي من خلال بعض الدول العربية (1) قبل تناول دور السياسة الجنائية في الحد من الجرائم الإلكترونية وأوجه القصور التشريعي (2).

1: المواجهة التشريعية في المغرب وبعض الدول العربية

تقوم أي سياسة جنائية على تحقيق غاية معينة تروم الحد من الظاهرة الإجرامية ومنها الجرائم الالكترونية، وهنا يطرح السؤال التالي: كيف واجه المشرع المغربي لهذه الجرائم؟ وهل كانت سياسته ناجعة في هذا المضمار؟

1 - أحمد عبد الله الالاه المراغي، الجريمة الالكترونية ودور القانون الجنائي في الحد منها، م س، ص 62و66و67.
2 علي جعفر ، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، م س ، ص 78و80و82.

1.1 المواجهة التشريعية في المغرب

تتميز الجريمة الإلكترونية بالسرعة والتطور والانتشار بشكل يتطابق وتطور وسائل التكنولوجيا الحديثة، وهذا الأمر يحتاج إلى قدرة كبيرة على مواكبة هذا التطور على مستوى التشريع أيضا، بحيث يكون مقابل كل فعل خبيث يحدث اضطرابا اجتماعيا نص تشريعي يجرمه ويعاقب عليه.

والجريمة الإلكترونية فرضت نفسها على المشرع المغربي لما تتسم به من خطورة و خصوصية، كما أن آليات هذه الجريمة لا تحتاج أكثر من مجرم له القدرة على توظيف خبرته في التعامل مع الوسائط التكنولوجية الحديثة لارتكاب الجريمة. فكان أن أصدر قانون 07.03 [1] بشأن مكافحة جرائم المس بنظم المعالجة الآلية للمعطيات ورسم نطاقه[2] .

كما وبالموازاة مع تطور الاجرام الإلكتروني وفي اطار حرص المشرع المغربي على مواكبة تطور النصوص القانونية الجنائية لهذا النوع من الإجرام فقد أصدر مؤخرا كما سبق الذكر، مجموعة القانون الجنائي في صيغة محينة بتاريخ 12 مارس 2018 وقد نص الفصل 447–1 من القانون الجنائي على عقوبات حبسية تتراوح بين ستة أشهر الى ثلاث سنوات وغرامة من (2000) الى (20000) درهم على كل من قام عمدا وبأي وسيلة بما في ذلك الأنظمة المعلوماتية بالتقاط أو تسجيل أو بث أو توزيع أقوال أو معلومات صادرة بشكل خاص أو سري دون موافقة أصحابها ويعاقب بنفس العقوبة ، من قام عمدا وبأي وسيلة، بتثبيت أو تسجيل أو بث أو توزيع صورة شخص أثناء تواجده في مكان خاص دون موافقته كما نص الفصل 2–447 على عقوبة بالحبس من سنة الى ثلاث سنوات وغرامة من (2000) الى (20000) درهم كل من قام بأي وسيلة بما في ذلك الأنظمة المعلوماتية ببث أو توزيع تركيبة مكونة من أقوال شخص أو صورته دون موافقته أو قام ببث أو توزيع ادعاءات أو وقائع كاذبة، بقصد المس بالحياة الخاصة للأشخاص أو التشهير بهم ، كما نص الفصل 3–447 على عقوبات مضاعفة في حالة ارتكاب الأفعال المنصوص عليها في الفصلين المذكورين في حالة العود وفي حالة ارتكاب الجريمة من طرف الزوج أو الطليق أو الخاطب أو أحد الفروع أو أحد الأصول أو الكافل أو شخص له ولاية أو سلطة على الضحية أو مكلف برعايتها أو ضد امرأة بسبب جنسها أو ضد قاصر.

1 - نص المشرع المغربي في مجموعة النصوص القانونية، القانون الجنائي المغربي وقانون الوقاية من الرشوة ومكافحة غسل الأموال، الطبعة الثانية 2008 في الباب العاشر في الفصول من3–607 الى غاية 11–607 ((على تحديد مفهوم نظم المعالجة الآلية للمعطيات ورسم نطاقه وعلى عقوبات حبسية متفاوتة حسب جريمة كل فصل تتراوح ما بين شهر الى خمس سنوات وغرامة مالية متفاوتة أيضا حسب جريمة كل فصل تبتدئ ما بين (2000) درهم الى (2.000.000) درهم ، دون الاخلال بالعقوبات الأشد أو التي ترفع الى الضعف اذا حصل عن الدخول الى مجموع أو نظام المعالجة الآلية للمعطيات حذف او تغيير أو اضطراب في سيره أو اذا مس ذلك معلومات تخص الأمن الداخلي أو الخارجي للدولة أو أسرارا تهم الاقتصاد الوطني ،كما يجوز الحكم ايضا وفق الفصول المذكورة على مصادرة الأدوات التي استعملت في ارتكاب الجرائم المنصوص عليها في هذا الباب والمتحصل عليه منها والحرمان من ممارسة واحد أو أكثر من الحقوق الوطنية أو المدنية أو العائلية المنصوص عليها في الفصل 40 من نفس القانون لمدة تتراوح بين سنتين وعشر سنوات، كما يمكن الحكم بالحرمان من مزاولة جميع المهام والوظائف العمومية لمدة تتراوح بين سنتين وعشر سنوات وبنشر أو بتعليق الحكم الصادر بالادانة))

2 - عبد السلام بنسليمان، الاجرام المعلوماتي في التشريع المغربي ،م س ، ص 133و137

ISSN: 7476-2605 ردمد

وفي نفس الصيغة المحينة لمجموعة القانون الجنائي المغربي في الفرع السادس منه تناولت الفصول من1-448 الى 14-448[1]. إحدى أخطر الجرائم المنظمة وهي جريمة بالاتجار بالبشر وخاصة اتجاه الأطفال الذين تقل سنهم عن ثمان عشرة سنة وخصها بعقوبات جنائية مشددة دون الإخلال بالمقتضيات الجنائية الأشد.

وفي الإصدار الجديد المذكور أدخل المشرع المغربي بعض الجرائم المتعلقة بالأخلاق الحميدة بواسطة التقنيات الحديثة للاتصال خصوصا مع انتشار عرض الصور الإباحية والخليعة ، ونشر صور شخصية للأفراد دون رضاهم وتحميلها بتعاليق مخلة بالحياء عدا عن فبركتها وإعادة التسجيل عليها وإعادة دمجها أوبث أو توزيع ادعاءات كاذبة أو وقائع كاذبة والتي تمس بخصوصية الأشخاص أو التشهير بهم.[2]

2.1 : المواجهة التشريعية في بعض الدول العربية.

جرم القانون الإماراتي "كل من تنصت أو التقط أو اعترض عمدا من دون وجه حق ، ما هو مرسل عن طريق الشبكة المعلوماتية أو احدى وسائل تقنية المعلومات بالحبس والغرامة أو بإحدى هاتين العقوبتين[3]

وذهب القانون السوداني الى القول " كل من يتنصت لأي رسائل عن طريق شبكة المعلومات أو الحاسوب أو ما في حكمه أو يلتقطها أو يعترضها دون تصريح بذلك من النيابة العامة أو الجهة المختصة أو الجهة المالكة للمعلومة، يعاقب بالسجن لمدة لا تتجاوز ثلاث سنوات أو بالغرامة.

كما عاقب المشرع السعودي على أفعال التنصت والاعتراض والالتقاط المعلوماتي "بالسجن لمدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ريال أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية: التصنت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي دون مسوغ نظامي صحيح أو التقاطه أو اعتراضه.

ونص المشرع العماني على أنه "يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على سنة وبغرامة لا تقل عن خمسمائة ريال عماني ولا تزيد على ألفي ريال عماني أو بإحدى هاتين العقوبتين، كل من اعترض عمدا ودون وجه حق باستخدام وسائل تقنية المعلومات خط سير البيانات أو المعلومات الإلكترونية المرسلة عبر الشبكة المعلوماتية أو وسائل تقنية المعلومات أو قطع بثها أو استقبالها أو التنصت عليها".

أما في دولة الجزائر فقد تناول المشرع في اطار التعديل الذي أجراه على قانون العقوبات الجزائري، جريمة الدخول أو البقاء بدون تصريح في النظام المعلوماتي وذلك في المادة(394)مكرر والتي تنص على أنه :"يعاقب بالحبس من ثلاثة أشهر الى سنة وبغرامة من (50.000)دج الى (100.000)دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. وتضاعف العقوبة

1 - ا مجموعة القانون الجنائي المغربي في صيغة محينة منشور على الموقع الالكتروني لوزارة العدل بالرباط. المغرب. بتاريخ 13 مارس2018.

2 - ولا شك أن المشرع المغربي قد أحسن صنعا حين تدخل ووضع حدا لمثل هاته الجرائم التي استفحل انتشارها في المجتمع وخاصة الماسة بالخصوصية ،وتلك الصادرة عن علاقة قرابة أو ضد امرأة بسبب جنسها أو ضد قاصر، وحتى تكون الأحكام القضائية من جانب آخر مرآة لهذه النصوص ،عدا عما سيتناوله الى جانبهم كل من الفقهاء والباحثين من تحليلات تكون لبنات أساسية لاصدار تشريعي مواكب للتطور الآني.

3 - ويلاحظ أن المشرع المغربي ونظرا لخطورة الأفعال المرتكبة وتحقيقا لمزيد من الردع لم يستعمل أثناء نصه على عقوبة الحبس والغرامة في الفصول1-477 الى 3-477 ما يفيد التخيير بين العقوبة الحبسية والغرامة أو باحددى هاتين العقوبتين ،على عكس بعض التشريعات:كالاماراتي والعماني والسوداني التي نصت أعلاه على عقوبة بالحبس والغرامة أو باحدى هاتين العقوبتين.

اذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة، واذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة بالحبس من ستة أشهر الى سنتين والغرامة من (50.000)دج الى (150.000) دج".

وتجدر الاشارة الى أن المشرع الجزائري لم يكتفي بتجريم الدخول أو البقاء بدون تصريح في النظام المعلوماتي بل تجاوز ذلك الى تجريم مجرد المحاولة وذلك بحسب العبارة الواردة في النص(أو يحاول ذلك) ، بما معناه تجريم الشروع في جريمة الدخول أو البقاء بدون تصريح في النظام المعلوماتي[1].

أما القانون العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها الصادر عن الأمانة العامة لجامعة الدول العربية بالرقم "417" فقد ذهب الى تجريم التنصت أو الالتقاط أو الاعتراض بدون وجه حق لما هو مرسل عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي أو ما في حكمها.[2] بعد ذلك يتم الانتقال الى دور السياسة الجنائية .

2: دور السياسة الجنائية وأوجه القصور التشريعي في الحد من الجرائم الالكترونية

يطرح موضوع البحث والتحقيق في الجريمة المعلوماتية اشكالات مهمة أنتجتها الطبيعة الخاصة والمعقدة لهذا الصنف من الاجرام وذلك بالنظر الى خصوصية المجرم المعلوماتي الذي ينتمي الى الفئة المتعلمة المحترفة في أغلب الأحيان والى القدرة التي يمتلكها في التحكم في تصرفاته وفي علاقاته بالغير الأمر، الذي يطرح صعوبة تعقبه من جهة والى وسائل ارتكاب الجريمة الالكترونية ،التي هي معدات متطورة لا يستوعبها الا المتخصصون ذوي الخبرة من جهة ثانية لذلك سيتم التطرق لكل من دور السياسة الجنائية في الحد من الجريمة الإلكترونية قبل عرض أوجه قصور هذه السياسة في الحد من الجرائم الإلكترونية.

1.2: دور السياسة الجنائية في الحد من الجريمة الإلكترونية.

قبل تناول دور التعاون الدولي وموقف الشريعة الاسلامية في الحد من الجريمة الإلكترونية ،لابد من عرض دور المجني عليه في الحد من لجريمة الإلكترونية

1.1.2: دور المجني عليه.

يساهم المجني عليه بقدر كبير في اكتشاف الجرائم التقليدية الا أن الأمر يبدو أكثر اختلافا في الجريمة الإلكترونية لأ ن المجني عليه غالبا ما يحجم عن الابلاغ عنها مما يترتب عن ذلك ظهور الرقم الأسود لهذه الجريمة والتي ترجع أسبابه إلى البيئة الإلكترونية والى خوف الضحايا:

فالبيئة الإلكترونية المعقدة التي ترتكب فيها الجريمة الإلكترونية، يصعب معها إمكان اكتشافها ومرد ذلك ما تتطلبه هذه الجريمة من خبرة خاصة وتدريب كافي لرجل البحث والتحري، فعدم الخبرة والتدريب لدى سلطات التحري والتحقيق في الجريمة الإلكترونية تدفع البعض إلى إدراجها ضمن الجرائم التقليدية مما يخلق بدوره عقبة أمام الدراسات الإحصائية التي تهدف إلى بيان حجم الجريمة.

1 - دلخار صلاح بوتاني، الحماية الجنائية الموضوعية، م س، ص 220و221.
2 - عمار عباس الحسيني ، جرائم الحاسوب والانترنت، الجرائم المعلوماتية، م س ، ص 337و338.

وإحجام الضحايا عن الإبلاغ بوقوع الجريمة الإلكترونية يمكن دره لأمرين ، الأول يتمثل في خشيتهم من خسارتهم للمستخدمين لديهم أو الثقة العامة من عملائهم، أو معرفة نقاط الضعف في الأنظمة المعلوماتية لغير الجاني. والأمر الثاني هو الخشية من التشهير والفضيحة وخاصة في الجرائم الماسة بالعرض والشرف.

وأمام الموقف السلبي للمجني عليه في الحد من الجريمة الإلكتروني فانه لا مناص إجراءات حمائية مادية وفنية :

ويؤخذ بعين الاعتبار في الأولى ، القائمون على العمل لأن المخاطر المحتمل حدوثها من قبلهم متنوعة وكثيرة ومن ثم يجب إجراء التحريات الأولية عنهم، وتدريب الموظفين والعاملين بالجهات المسؤولة بكيفية منع وقوع الجريمة الإلكترونية .

بينما إجراءات التأمين الفنية تتمثل في إمدادهم بالوسائل الفنية التقنية عن طريق إلزام الشركات المنتجة للبرامج بوضع العراقيل للحيلولة دون دخول المتلصصين أو القراصنة إلى تلك البرامج، كذلك يمكن لهذه الشركات إعداد برامج للكشف عن هوية القراصنة وأماكن دخولهم إلى الشبكة، وذلك أولا بواسطة استخدام كلمات السر الخاصة، وثانيا استخدام التشفير والذي يعد وسيلة هامة ورئيسية إلى جانب الرقم السري أو كلمة المرور، لحماية رسائل البيانات والمعلومات المتبادلة بالطريق الإلكتروني حيث يحول التشفير المعلومات المقروءة إلى معلومات غير مقروءة عن طريق استخدام معادلات رياضية ولوغر يتمات معقدة. ويتم فك التشفير باستخدام برنامج مماثل عند استقبال المعلومات المشفرة . كما يعد التوقيع الإلكتروني من أهم الوسائل للحماية الفنية التكنولوجية الحديثة في حماية أمن المعلومات والبيانات بالإضافة الى التأمين باستخدام الجدران النارية وهي عملية تقوم بمسح المعلومات التي تصل من شبكة الأنترنت، وتحليلها ،وفي حالة الشك في أي من تلك المعلومات بوجود محاولة للدخول أو اختراق إحدى المناطق المؤمنة يقوم الجدار الناري بمنع هذه المحاولة أو طردها خارج الشبكة ثم يقوم بإصدار إنذار عن طريق إشارات يصدرها عن وجود مثل تلك المحاولات ويبدأ في تتبع المصدر لمعرفة صاحبه.[1]

2.1.2: دور التعاون الدولي وموقف الشريعة الإسلامية في الحد من الجريمة الإلكتروني.

التعاون الدولي :أدركت دول العالم الطبيعة الدولية للجرائم الإلكترونية التي تمثل الجريمة المنظمة إحدى صورها المختلفة والتي يمتد فيها مسرح الجريمة عبر عدة دول، الأمر الذي يترتب عليه عرقلة إعمال التحري والتحقيق وجمع الأدلة اللازمة لإدانة الجناة أمام القضاء لاصطدام تلك الأعمال والإجراءات بحدود السيادة الوطنية للدول الأخرى[2].

لذلك بات ملحا مواجهة الجريمة الإلكترونية بواسطة التعاون الدولي ، ولعل أبرز الجهود الدولية في هذا الإطار توقيع اتفاقيات دولية تعالج الجرائم الإلكترونية منها على سبيل المثال اتفاقية مجلس أروبا بشأن الإجرام السيبيري لسنة 2001 وهي الاتفاقية الوحيدة المتعددة الأطراف المعنية بمكافحة الجرائم التي تتم

1 - أحمد عبد اللاه المراغي، الجريمة الالكترونية ودور القانون الجنائي في الحد منها، م س ، ص من 117و122

2 - شاكر ابراهيم العموش، المواجهة الجنائية لجرائم الاتجار بالبشر،دراسة مقارنة،الطبعة الأولى نالدا العلمية الدولية،الأردن2016 ،ص452

باستخدام أو ضد الكمبيوتر باستخدام شبكة الأنترنت، وهي تمثل ركيزة أساسية منذ دخولها حيز النفاذ في الأول من يوليو 2004 على مستوى الدول أعضاء مجلس الاتحاد الأروبي، وقد وقعت عليها العديد من الدول من غير أعضاء مجلس أروبا مثل كندا واليابان وجنوب افريقيا كما صادقت عليها الولايات المتحدة الأمريكية.

وإن الجرائم الإلكترونية تختلف كثيرا بالنسبة للجرائم المتعارف عليها في القانون الجنائي كالسرقة والقذف والقتل وغيرها ،كما أن التعامل معها من خلال البحث والتحقيق وجمع الأدلة صعب جدا، ولا شك أن التكنولوجيا الحديثة تقدم للدول وأجهزتها الأمنية الكثير من التسهيلات والإمكانات التي تسهم في رفع كفاءاتها وتطوير قدرتها على التصدي للجريمة، إلا أن هذا التطور التكنولوجي أدى ويؤدي في الوقت نفسه إلى تطوير وتحديث الجريمة من حيث الأساليب والمضامين، فالإعلام الآلي الذي ارتقى بمستوى الانسان وانتقل به إلى عصر المعلوماتية والتقدم هو ذاته الذي يستخدمه بارونات الجريمة الإلكترونية وعصابات المافيا ، وقد يساهم أكثر من شخص في دول مختلفة في ارتكاب جريمة واحدة يقع ضحيتها عديد من الأفراد يقيمون في بلدان متعددة، فتظهر مشكلة التعارض والاختلاف بين التشريعات الإجرائية في دول العالم، ومنها اختلاف الجهات المختصة بالتفتيش، ومكافحة الجرائم الإلكترونية تقتضي إذا توحيد التشريعات الإجرائية من ناحية، وأن يكون نظام الإثبات بالدليل الإلكتروني واحدا بين الدول التي تقع فيها هذه الجرائم وهذا أمر مستحيل تحقيقه.

لذلك كان لابد أن يكون هناك تعاون دولي يتفق مع طبيعة هذه الجرائم ويسمح هذا التعاون الدولي بسهولة الاتصال المباشر بين أجهزة الشرطة في الدول المختلفة. والدولة وحدها لا تستطيع القضاء على هذه الجرائم، وتتولى المنظمة الدولية للشرطة الجنائية اقامة العلاقات بين دول المنظمة وتبادل المعلومات بين سلطات التحقيق. لذلك فان ملاحقة مرتكبي هذه الجرائم وتقديمهم للمحاكمة وتوقيع العقاب عليهم يستلزم القيام بأعمال اجرائية أو ضبط الأقراص الصلبة التي توجد عليها معلومات غير مشروعة قانونا أو صور إباحية، أو تفتيش الوحدات الطرفية في حالة الاتصال عن بعد أو القبض على الاظناء أو سماع الشهود ،أو اللجوء الى الانابة القضائية ، أو تقديم المعلومات التي يمكن أن تساهم في تحقيق هذه الجرائم[1].

أما موقف الشريعة الاسلامية في الحد من الجريمة الإلكترونية، فإنه وما دامت شبكة الأنترنت وأمثالها من النظم المستحدثة، فإن ذلك لا يعني أن الشريعة ترفضها وتبعدها، على العكس مادام هناك فوائد تعود على البشرية من خلال هذه التقنية فان الشريعة الإسلامية تدعو إليها، ذلك أن تعظيم الشريعة للعلم النافع أمر تحبذه الشريعة والنصوص في ذلك كثيرة ومشهورة سواء كانت نصوصا قرآنية[2] أو أحاديث نبوية.

وتقنية الأنترنت لها فوائد جمة وعظيمة وما دام للتقنية فائدة فإنها لا ترفضها، ويقال هنا أن "دفع المفاسد مقدم على جلب المصالح" وهذه التقنية فوائدها جلية وعظيمة والمفسدة تأتي من خلال استغلال التقنية الاستغلال السيء إلا أنها نفع في ذاتها، ذلك لو قلنا بذلك" دفع المفاسد" لما أخذنا بأي تقنية علمية، لأنه ما من اكتشاف موجود إلا وله أضرار مثلما له فوائد، لذا لزم اذا كان فعل الفرد يشكل جريمة من الجرائم فإن فعله

1 - أحمد عبد اللاه المراغي، الجريمة الالكترونية ودور القانون الجنائي في الحد منها، م س ، ص125و128

2 - الآية 33 من سورة الرحمان " يا معشر الجن والانس ان استطعتم أن تنفذوا من أقطار السماوات والأرض فانفذوا لا تنفذون الا بسلطان"

ISSN: 7476-2605 ردمد

هذا يجب أن يعاقب عليه، ويتضح أن نظرية العقاب في الشريعة الاسلامية غاية في المرونة ذلك أن نظام التعزير يصلح لكل زمان ومكان، ما لم يكن الفعل يشكل جريمة حد أو قصاص[1].

2.2: القصور التشريعي في الحد من الجريمة الإلكترونية

رغم المجهودات المبذولة من قبل التشريعات في مكافحة الالكترونية على الصعيد الدولي فما زالت توجد مواطن القصور لديها، مما تحتاج إلى المزيد من الاهتمام كما سيبين بعده.

1.2.2 : القصور التشريعي من خلال الجهود الدولية

إن بطء الاجراءات الرسمية يجازف غالبا بفقدان الأدلة، وقد تكون بلدان متعددة متورطة في الأمر، ولذلك تشكل متابعة وحفظ سلسلة الأدلة تحديا كبيرا ،بل حتى في الجرائم المحلية، قد يكون لها بعد دولي، وربما تكون هناك حاجة إلى طلب المساعدة بين البلدان التي مرت الهجمة من خلالها، وإذا كانت هناك جريمة واضحة تستحق التحقيق بالفعل فقد تكون هناك حاجة إلى طلب مساعدة من السلطات في البلد الذي كان منشأ الجريمة أو من السلطات في البلد أو البلدان التي عبر من خلالها النشاط المجرم وهو في طريقه إلى الهدف، أو حيث قد توجد أدلة الجريمة .وهناك عنصران أساسيان للتعاون : المساعدة غير الرسمية من محقق لآخر، والمساعدة الرسمية المتبادلة.

وقد تكون المساعدة غير الرسمية أسرع انجازا وهي الوسيلة المفضلة في النهج حين لا تكون هناك صلاحيات إلزامية(أي أوامر تفتيش أو طلب تسليم المجرم)،ومن ناحية أخرى فإن المساعدة الرسمية المتبادلة هي عملية أكثر إرهاقا يتم اللجوء إليها عادة بترتيبات لمعاهدات بين البلدان المعنية. ومن بين بعض أوجه القصور التشريعي :

أولا عدم وجود نموذج موحد للنشاط الإجرامي، فليس هناك اتفاق مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات وشبكة الأنترنت الواجب تجريمها، فما يكون مباحا في أحد الأنظمة قد يكون مجرما وغير مباح في نظام آخر ويمكن إرجاع ذلك لعدة أسباب وعوامل كاختلاف البيئات والعادات والتقاليد والديانات والثقافات من مجتمع لآخر.

وثانيا في تنوع واختلاف النظم القانونية الإجرائية، وكذا يرجع إلى عدم وجود قنوات اتصال بجهات أجنبية لجمع أدلة معينة بالإضافة الى التنازع في الاختصاص بين الدول. فقد يحدث أن ترتكب الجريمة في إقليم دولة معينة من قبل أجنبي ، فهنا تكون الجريمة خاضعة للاختصاص الجنائي للدولة الأولى استنادا إلى مبدأ الاقليمية ، وتخضع كذلك لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي في جانبيه، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى فتدخل عندئذ في اختصاصها استنادا إلى مبدأ العينية ، وكذلك تطرح فكرة تنازع الاختصاص القضائي في حالة تأسيس الاختصاص على مبدأ الإقليمية ، كما لو قام الجاني ببث الصور الخليعة ذات الطابع الإباحي من إقليم دولة معينة وتم الاطلاع عليها في دولة

1 - أحمد عبد اللاه المراغي، الجريمة الالكترونية ودور القانون الجنائي في الحد منها، م س ، ص141

أخرى ففي هذه الحالة يثبت الاختصاص وفقا لمبدأ الاقليمية لكل دولة من الدول التي مستها الجريمة إلى غير ذلك من الصعوبات المتعلقة بالإنابات القضائية الدولية في المجال الجنائي والتي من أهم صورها أن تسلم بالطرق الدبلوماسية وهذا طبعا يجعلها تتسم بالبطء والتعقيد ،وكذا الصعوبات المتعلقة بالتعاون الدولي في مجال التدريب والتي تتمثل في عدم رغبة بعض القيادات الإدارية في بعض الدول في التدريب لاعتقادهم بدوره السلبي في تطوير العمل من خلال تطبيق ما تعلمه المتدربون في الدورات التدريبية وما اكتسبوه من خبرات إلى عير ذلك من الصعوبات والتي تؤثر سلبا على مكافحة الجرائم الإلكترونية[1].

2.2.2: القصور التشريعي من خلال بعض التشريعات

في محاولة للوقوف على بعض أوجه القصور التشريعي في كثير من الدول العربية والتي تحول دون الملاحقة الجنائية لمرتكبي الجرائم الإلكترونية يمكن الإشارة إلى مبدأ الشرعية الجنائية الذي يفرض عدم جواز التجريم والعقاب عند انتفاء النص، لذا يتعين على المشرعين في سائر الدول العربية مواكبة التطورات التي حدثت في المجتمعات الأخرى، وسن التشريعات اللازمة للتصدي لظاهرة الاجرام الإلكتروني[2].

ورغم صعوبة ضبط وصعوبة مكافحة الجرائم الالكترونية على الصعيد العربي إلا أن هناك جهودا جماعية وفردية في محاربة قراصنة الأنترنت وإحالتهم قانونا على المحاكم ، ولكن هذه الجهود فيها ما هو مضاد لحرية التعبير ويمكن ان نذكر من بين الجهود الجماعية العربية، ما حصل من تعاون عربي في هذا الصدد بمناسبة انعقاد "مؤتمر وزراء الداخلية العرب في تونس سنة 2006" عندما قدم وزير الداخلية المصري اقتراحا بتوحيد الجهود العربية للعمل على استصدار قرار من مجلس الأمن بالتزام الدول التي تتبعها المؤسسات، والشركات العالمية الكبرى التي تباشر إدارة واستقبال شبكات المعلومات والاتصال، بإغلاق المواقع التي تبث بيانات للأفكار والأيديولوجيات المتطرفة، قد قوبل هذا المطلب بمواجهة عنيفة من قبل المنظمات الحقوقية التي اعتبرت مثل هذا الإجراء ما هو الا تقييد لحرية الرأي والتعبير.

كما تحركت مصر والسعودية مرة أخرى في مؤتمر وزراء الإعلام العرب سنة 2008 "بتقديم مسودة مشروع مقترح لتشكيل لجنة عليا للإعلام الإلكتروني" وهو خطوة أخرى ظاهرها مكافحة الجرائم الإلكترونية وباطنها هو تقييد حرية الرأي والتعبير، مستندين على أن الإعلام الإلكتروني في الدول العربية يتسم بالخطورة ولا تحكمه أية معايير أو ضوابط مهنية واضحة يمكن الإلزام بها [3]

خاتمـــــــة:

أدى التطور التكنولوجي إلى ظهور أنماط مستحدثة من الأفعال الجرمية ،وبالمقابل فإن التشريعات على اختلافها دولية ووطنية كلما سارعت إلى تدارك حقبة معينة لظهور جرائم مختلفة على مستوى إلكتروني، بتطوير قوانينها الجنائية أو تحيينها بما قد يحد من نوعية هذه الجرائم إلا وتعقبها جرائم أخرى أكثر تطورا،

1 - يوسف حسن يوسف، الجرائم الدولية للانترنت، م س ، ص185و190

2 - المرجع السابق، ص296

3 - المرجع السابق، ص 271.

وأكثر مسألة تثير التساؤل هي مسألة تحديد أنماط السلوك الإجرامي والأفعال المكونة له، وتوضيح العناصر المكونة لهذه الجرائم الإلكترونية،كما وان ما يؤخذ على القوانين الجنائية المواكبة لهذا التطور هو استناد أغلبها خاصة في بعض الدول العربية ، على قوانين إجرائية تقليدية أضحت غير مسعفة مما يطرح جذلا حول مقبولية المخرجات كإثبات جنائي أمام القاضي الجنائي ،ما دام المشرع لم يحدد القانون الإجرائي الموازي له ولم يحدد شخص القائم بالمخرجات قانونا بجميع الشكليات المتطلبة لتلك المخرجات وللجهاز الإلكتروني موضوع ارتكاب الجريمة من ناحية قانونية صرفة حتى يمكن ممارسة المساطر القانونية والطعن فيها أمام القضاء سواء على مستوى وطني أو دولي باعتبار هذه الجرائم عابرة للقارات. وأمام هذا الفراغ التشريعي فلا مناص من التأكيد على الدور الهام للسلطة التقديرية للقاضي الجنائي .



وأمام عدم وجود تشريع جنائي عربي موحد يجرم صور وأنواع الجرائم الإلكترونية، فلا بد وتكثيف الجهود وإبرام اتفاقيات ومعاهدات خاصة بهذا النوع من الجرائم على الصعيدين العربي والدولي.